System Name: eCampus-Based System (eCB)

Principal Office: Office of Federal Student Aid (FSA)

C&A Document: Configuration Management Plan (CMP)

Purpose: The table that follows contains the results of a review performed on the eCB CMP. The CMP was assessed against the criteria outlined in the source document(s) referenced below. The observations in the table identify items within the CMP that do not completely meet the criteria. For each observation, a recommendation is provided that is intended to provide guidance for improving the document prior to formal submission to the Certification Review Group (CRG). Note that implementation of recommendations does not guarantee that the CMP will pass the CRG review criteria. The recommendations section of the table is designed to: ensure consistency, provide clarification of meaning, reduce gaps in content, and enhance quality. Sections of the document that were found to adequately and sufficiently meet the criteria discussed above are not listed below to conserve space and efficiency; only those sections that did not meet the criteria are listed in the table.

Observation Categories: To assist in categorizing comments by type, a three-tier color-coding scheme is applied. Green indicates that the observation is not substantial enough to impact the overall quality and substance of the document's content and implementing the suggested recommendations is not critical. Yellow indicates that while the document essentially meets the criteria, in our opinion, additional information will help the assessor better evaluate the extent of compliance. Red indicates that the observation is substantial enough to impact the overall quality of the document's content and it is failing to meet the functional intent of the governing standards. All Red and Yellow observations must be corrected to ensure the governing standards are met.[1] If you non-concur with any of the observations, request a meeting so that any issues and concerns can be resolved and documented in the corrective action plan.

Criteria Source: *Department of Education Handbook for IT Security Configuration Management Planning Procedures* and Tier 1 & 2 CMP Template

Scope: This evaluation primarily focused on the content outlined within the body of the CMP. Note that in some cases there are varied solutions, approaches, or alternatives to addressing the observation.

General Observation: Based on the documentation analysis performed, it was determined there are several areas that have not been adequately addressed within this CMP. There are 16 Red observations that have been categorized as substantial and should receive high priority and 6 Yellow observations that need additional information to ensure compliance.

[1] *Per Section 3.1.3.2 of the Handbook for IT Security Certification and Accreditation Procedures - " High and medium risks must be mitigated in order for a GSS or MA to be certified."*

No.		Section/Page	Observations	Recommendations	Corrective Actions Proposed	Due Date for Corrections
1.	Yellow	1.3 Scope Reference p. 3	This section does not clearly state the scope of the CMP.	Update this section by providing the scope of the CMP as it relates to the system. Refer to the template for example language for this section.	Will update the plan to include the scope.	2/12/04
2.	Red	1.4 Structure	This section is not included in the CMP.	Include this section and provide the structure of the document. Refer to the template for example language for this section.	Will add a paragraph explaining the structure of the document.	2/12/04
3.	Yellow	2. Roles and Responsibilities Reference p. 3-5	This section describes the roles and responsibilties of those involved in the CM process for the system; however, the role and responsibility of the CIO has not been provided.	Update this section by providing the role and responsibility of the CIO as it relates to the CM of the system. Refer to the template for example language for this section.	Will add the CIO role, as per the template language.	2/12/04
4.	Red	4.1.1 Purpose and Functionality	This section is not included in the CMP.	Include this section and provide a description of the purpose and functionality of the system. Refer to the template for example language for this section.	Will add system description language from the System Security Plan (SSP)	2/12/04
5.	Red	4.1.2 Users	This section is not included in the CMP.	Include this section and provide a description of the users of the system. Refer to the template for example language for this section.	NOTE: The configuration management plan is included as an appendix to the eCB System Security Plan. Therefore, many of the comments regarding section 4 will be addressed by referring readers to the appropriate section of the SSP. Will make a reference to the appropriate section of the SSP.	2/12/04
6.	Red	4.1.3 System Criticality	This section is not included in the CMP.	Include this section and provide the criticality of the system and the justification for the assigned rating. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04

No.		Section/Page	Observations	Recommendations	Corrective Actions Proposed	Due Date for Corrections
7.	Red	4.1.4 Data Sensitivity	This section is not included in the CMP. This is provided in the attached guidance.	Include this section and provide the overall sensitivity of the system. Refer to the attached guidance as well as the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
8.	Red	4.1.4.1 System Confidentiality	This section is not included in the CMP.	Include this section and provide the justification for the confidentiality rating of the system. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
9.	Red	4.1.4.2 System Integrity	This section is not included in the CMP.	Include this section and provide the justification for the integrity rating of the system. Refer to the template for example language for this section.	Unclear—do you mean “data integrity”? If so, will make a reference to the appropriate section of the SSP.	2/12/04
10.	Red	4.1.4.3 System Availability	This section is not included in the CMP.	Include this section and provide the justification for the availability rating of the system. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
11.	Red	4.1.5 Data	This section is not included in the CMP.	Include this section and provide a description of the specific type of data being processed by the system. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
12.	Red	4.2 System Architecture	This section is not included in the CMP.	Include this section and provide a diagram and a detailed description of the architecture of the system. Refer to the template for an example diagram and language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
13.	Red	4.3 Hardware	This section is not included in the CMP.	Include this section and provide the hardware components of the system. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04

No.		Section/Page	Observations	Recommendations	Corrective Actions Proposed	Due Date for Corrections
14.	Red	4.4 Software	This section is not included in the CMP.	Include this section and provide the software components of the system. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
15.	Red	4.5.1 System Documentation	This section is not included in the CMP.	Include this section and provide a list of security documentation for the system. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
16.	Yellow	5.3 Step 3: Evaluate Change Request Form Note: Information found in Appendix A	This section provides information on the evaluation of change requests; however, the criteria used for evaluating a change request is not adequately described.	Update this section by addressing the criteria used to evaluate a change request. Refer to the template for example language for this section.	Partial nonconcur: Covered in Appendices A and B. However, will add some general language to the body of the text and refer readers to appendices.	2/20/04
17.	Yellow	5.5 Step 5: Approve, Disapprove, Defer, Refer Change Request Note: Information found in Appendix A	This section provides general information on the approval of a change request; however, no specific information has been provided regarding the actual approval, disapproval, deferment, or the referral of change requests.	Update this section by providing the steps used for approving, disapproving, deferring, and referring a change request and what these decisions consist of. Refer to the template for example language for this section.	Will update CMP with modified template language.	2/20/04
18.	Yellow	5.6 Step 6: Test and Implement Approved Change Request Note: Information found in Appendix C	This section does not include the specific steps used to test a change request prior to implementation.	Update this section by providing a detailed description of the steps used to test a change request prior to implementation. Refer to the template for example language.	Partial nonconcur: Covered in Figure 2. Will add modified template language saying who is responsible for testing.	2/20/04
19.	Red	5.8 Step 8: Conduct Configuration Verification and Audit	This section is not included in the CMP.	Include this section and provide a description of how configuration verification and auditing are conducted and what each consists of. Refer to the template for example language.	Partial nonconcur: Basic flow of events covered in pages 13-14. Will add some modified information from the template.	2/20/04

No.		Section/Page	Observations	Recommendations	Corrective Actions Proposed	Due Date for Corrections
20.	Red	6.1.1 Physical Controls	This section is not included in the CMP.	Include this section and provide a description of the physical security controls implemented at the facility where the system is housed. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
21.	Red	6.1.2 Environmental Security Controls	This section is not included in the CMP.	Include this section and provide a description of the environmental security controls implemented at the facility where the system is housed. Refer to the template for example language for this section.	Will make a reference to the appropriate section of the SSP.	2/12/04
22.	Yellow	6.3 Development Environment Note: Information found in Appendix B	This section provides general information on the development environment of the system; however, no specific information detailing the hardware and software used, configuration, and safeguards implemented has been provided.	Update this section by providing a detailed description of the development environment to include; the hardware and software components used, their configuration, and the safeguards implemented to ensure that corrupted files are not introduced into the production environment. Refer to the template for example language for this section.	Will add a paragraph in the existing development/testing section to address these concerns.	2/20/04

Additional Comments:

(1) Spell out all acronyms used throughout the document and update Appendix A.
(2) Proof-read the document for spacing and formatting inconsistencies.